5 Structure of 2-transitive groups

THEOREM 5.1 *(Burnside) Let G be a 2-transitive permutation group on a set Ω. Then G possesses a unique minimal normal subgroup N and one of the two options occurs:*

1. *N is regular, elementary abelian, and G is permutation isomorphic to a subgroup of an affine group $\mathrm{AGL}(d, \mathbb{Z}_p)$ acting naturally on $\mathbb{Z}_p^d$ with G_ω being a subgroup of $\mathrm{GL}(d, \mathbb{Z}_p)$ acting transitively on the non-zero vectors in $\mathbb{Z}_p^d$.*
2. *N is a non-abelian simple group acting primitively on Ω.*

PROOF. Let N be a minimal normal subgroup of G. Since N is a non-trivial normal subgroup of a primitive group, it is transitive. If N is not the unique minimal normal subgroup of G, then, by Theorem 4.6, the only other minimal normal subgroup is the centraliser $C_G(N)$, and both N and $C_G(N)$ are regular non-abelian normal subgroups of G. However, a regular normal subgroup of a 2-transitive group is elementary abelian, a contradiction. This shows that N is the unique minimal normal subgroup of G.

If N is regular, then, as above, it is elementary abelian and (1) holds. Suppose thus that N is not regular.

Suppose first that N is imprimitive and let B be a minimal non-trivial block of imprimitivity for N. Let $\mathcal{B} = \{B^g : g \in G\}$. Since N is normal in G, each element of $\mathcal{B}$ is a minimal block of imprimitivity for N. (Why?!) Since an intersection of two blocks is again a block, it follows that any two elements of $\mathcal{B}$ intersect in at most one element.

Since B is not trivial, there exists two elements $\omega, \delta \in B$. Now take any $\omega', \delta' \in \Omega$. Since G is 2-transitive, there exist $g \in G$ such that $\omega^g = \omega'$ and $\delta^g = \delta'$, and thus $\omega', \delta' \in B^g$. Together with what we proved above, this shows that for any two elements of $\omega, \delta \in \Omega$, there exists a unique block in $\mathcal{B}$ containing them; we shall denote this block by $[\omega\delta]$.

We will now show that $N_{\omega\delta} = 1$ for any two $\omega, \delta \in \Omega$. Since each element of $\mathcal{B}$ is a block of imprimitivity for N, it follows that N_ω fixes (set-wise) every block through ω. Now let $g \in N_{\omega\delta}$ and let γ be an element of Ω not contained in $[\omega\delta]$. Then $N_{\omega\delta}$ fixes set-wise $[\omega\gamma]$ as well as $[\delta\gamma]$, thus fixing their intersection, which is γ. In particular, $N_{\omega\delta} \le N_{\omega\gamma}$ for any $\gamma \in \Omega \setminus [\omega\delta]$. But then (by switching the roles of γ and δ), it follows that $N_{\omega\gamma}$ (and thus also $N_{\omega\delta}$) fixes every point not contained in $[\omega\gamma]$, and therefore every point on $[\omega\delta]$. In particular, $N_{\omega\delta} = 1$, as claimed.

We have thus shown that N is a Frobenius group. We could now use the Frobenuis theorem to show that N contains a characteristic regular normal subgroup R, consisting of the identity and all fixed-point-free elements of N. Such a group would then be normal in G, and by minimality of N, we would have $N = R$, implying that N is regular itself, which contradicts out assumptions. Alternatively, to avoid appealing to the proof of the Frobenius theorem, we could continue in a more elementary way, which can be outlined as follows (you will be required to fill in details as a part of 2nd Assignment):

Let R^* be the set of all fixed-point-free elements of N and let $R = R^* \cup \{1\}$. Prove that $|R| = n$, where $n = |\Omega|$. Use this to argue that for any two $\alpha, \beta \in \Omega$ there is a unique $g \in R^*$ mapping α to β. Now use 2-transitivity of G to conclude that all elements in R^* are conjugate within G. Now let p be a prime dividing n, and P a Sylow p-subgroup of N. Then P contains a fixed-point-free element of order p. So all elements in R^* have order p, and n is a power of p. Then it follows that P is transitive (why?), and so consists of the identity and all the elements in R^*; in particular, $P = R$, and thus R is a regular normal subgroup of G. Since R is regular and G primitive, R is minimal, and thus $N = R$, a contradiction.

Either way, we proved that whenever N is imprimitive, it is regular, and thus part (1) holds. Suppose now that N is primitive but not regular. Being a minimal normal subgroup of G, $N = T_1 \times \ldots \times T_k$, where T_i are minimal normal subgroups of T, all isomorphic to some fixed normal non-abelian (why non-abelian?!) simple group T. On the other hand, N is primitive so either contains a unique minimal normal subgroup (and thus $k = 1$) or it contains two distinct mutually centralising minimal normal subgroups—both regular (here $k = 2$).

We are thus left with the case where the unique minimal normal subgroup N is a direct product $T \times S$, where T and S are isomorphic, both regular, they centralise each other and are non-abelian simple. Moreover, and element of G either normalises both S and T or conjugates one to the other. Let $\tilde{G}$ be the normaliser of N in $\mathrm{Sym}(\Omega)$. Then $G \leq \tilde{G}$ and hence $\tilde{G}$ is 2-transitive. By definition, N is normal in $\tilde{G}$, and since N is minimal normal in G, so it is in $\tilde{G}$. By what we showed, N is the unique minimal normal subgroup of $\tilde{G}$. Now let $\tilde{H}$ be the normaliser of T in $\tilde{G}$; note that $\tilde{H}$ is the kernel of the action of $\tilde{G}$ on $\{T, S\}$ by conjugation and thus $|\tilde{G} : \tilde{H}| = 2$; also $N \leq \tilde{H}$. Hence T is a regular normal subgroup in a primitive group $\tilde{H}$, hence, without loss of generality, $\Omega = T$ and $\tilde{H} \cong T \rtimes \tilde{H}_1$, in its natural action on T. Now recall that S is the centraliser of T in $\mathrm{Sym}(\Omega) = \mathrm{Sym}(T)$. But the group L of permutations $\lambda_g \colon t \mapsto g^{-}t$, $g \in T$, also centralises T and acts regularly on

T. Hence $S = L$, and thus $N = L \times T$. But the permutation $\iota \in \mathrm{Sym}(T)$, $g \mapsto g^{-1}$, conjugates S to L and vice versa, and thus belongs to $\tilde{G} \setminus \tilde{H}$. In particular, $\tilde{G} = \langle \tilde{H}, \iota \rangle$. Also, since ι fixes $1 \in T$, it follows that $\tilde{G}_1 = \langle \tilde{H}_1, \iota \rangle$. Now, both ι and elements of $\tilde{H}_1$ preserve the order of elements in T (the latter being acting as conjugations), implying that $\tilde{G}_1$ preserves the orders of elements in T. But $\tilde{G}_1$ (being 2-transitive) acts transitively in $T \setminus \{1\}$, implying that T is an elementary abelian p groups, a contradiction.

6 Permutation groups of prime degree

THEOREM 6.1 *(Burnside) Let G be a transitive permutation group on a set Ω of prime size p. Then either G is doubly transitive or G is permutation isomorphic to a group $\tilde{G}$ satisfying $\mathbb{Z}_p \le \tilde{G} \le \mathrm{AGL}(1, \mathbb{Z}_p)$.*

Throughout this section, let $\mathbb{F} = \mathbb{Z}_p$, the field of order p, and let $\mathbb{F}^\Omega$ denote the set of all functions from Ω to $\mathbb{F}$. If we endow $\mathbb{F}^\Omega$ with the point-wise addition and multiplication with scalars from $\mathbb{F}$, it becomes an $\mathbb{F}$-vector space. For $\omega \in \Omega$, let $\chi_\omega \in \mathbb{F}^\Omega$ be the characteristic function of ω. Then $\{\chi_\omega : \omega \in \Omega\}$ is clearly a basis for $\mathbb{F}^\Omega$.

Now let G act upon $\mathbb{F}^\Omega$ according to the rule:

$$f^g(\omega) = f(\omega^{g^{-1}}), \text{ for all } f \in \mathbb{F}^\Omega, g \in G \text{ and } \omega \in \Omega.$$

Observe that for each $g \in G$, the mapping $T_g \colon \mathbb{F}^\Omega \to \mathbb{F}^\Omega$, $T_g \colon f \mapsto f^g$ is in fact an invertible linear transformation of the $\mathbb{F}$-vector space $\mathbb{F}^\Omega$. Moreover, the mapping $G \mapsto \mathrm{GL}(\mathbb{F}^\Omega)$, $g \mapsto T_g$, is an injective group homomorphism. In particular, by identifying g with T_g, we may view G as a subgroup of $\mathrm{GL}(\mathbb{F}^\Omega)$. (CHECK ALL THIS!)

Further, let $\mathrm{Hom}(\mathbb{F}^\Omega, \mathbb{F}^\Omega)$ (denoted in short by Hom) be the $\mathbb{F}$-linear space of all linear transformations of $\mathbb{F}^\Omega$, and let $\mathrm{Hom}_G(\mathbb{F}^\Omega, \mathbb{F}^\Omega)$ (denoted in short by Hom_G) be the set of all those $\varphi \in \mathrm{Hom}$ that commute with every $g \in G$. That is, $\varphi \in \mathrm{Hom}_G$ if and only if $\varphi(f)^g = \varphi(f^g)$ for every $g \in G$ and $f \in \mathbb{F}^\Omega$. (CHECK THAT THIS IS INDEED A SUBSPACE OF Hom.)

Note (CHECK!) that for $g \in G$ and $\omega \in \Omega$, we have

$$(\chi_\omega)^g = \chi_{\omega^g}$$

and deduce that, for a fixed $\omega \in \Omega$, the mapping $\Phi \colon \mathrm{Hom}_G \to \mathbb{F}^\Omega$, $\Phi \colon \varphi \to \varphi(\chi_\omega)$ is injective and $\mathbb{F}$-linear. In particular, the dimension of Hom_G (as an $\mathbb{F}$-vector space) equals the dimension of the subspace $\Phi(\mathrm{Hom}_G)$ of $\mathbb{F}^\Omega$.

Now prove that $f \in \Phi(\mathrm{Hom}_G)$ if and only if f is constant on each G_ω-orbit on Ω. Use this do deduce the following lemma:

LEMMA 6.2 *Let $\omega \in \Omega$.Then $\dim_{\mathbb{F}}$ Hom_G equals the number of orbits of G_ω on Ω.*

We will also need the following lemma:

LEMMA 6.3 *Let $\mathbb{F}$ be a finite field of order p. Then, for every function $f \colon \mathbb{F} \to \mathbb{F}$ there exists a unique polynomial $\pi_f \in \mathbb{F}[x]$ of degree at most $p-1$ such that π_f and f coincide as functions on $\mathbb{F}$.*

Let us now prove Burnside's theorem. The theorem clearly holds for $p = 2$ and 3 (A WORD OF EXPLANATION). So we shall assume that $p \geq 5$.

Let g be an element of order p in G and let $P = \langle \rho \rangle$ (PROVE THAT P is in fact the Sylow p-subgroup of G). Since we want to determine the group G only up to permutation isomorphism, we may assume that $\Omega = \mathbb{F}$ and $\rho\colon \alpha \to \alpha - 1$ for every $\alpha \in \mathbb{F}$.

In view of Lemma 6.3, we may identify $\mathbb{F}^{\mathbb{F}}$ by the $\mathbb{F}$-vector space $\mathbb{F}_{p-1}[x]$ of polynomials of degree at most $p-1$. In view of this identification, we may thus view ρ as the polynomial $x - 1$.

Recall that G can be viewed as a group of linear transformations of the vector space $\mathbb{F}^{\Omega}$ $(= \mathbb{F}^{\mathbb{F}} = \mathbb{F}_{p-1}[x])$. It thus makes sense to ask which subspaces of $\mathbb{F}^{\Omega}$ are G-invariant (preserved by G). In fact, in order to prove the theorem, we need to show that the subspace of linear transformations $\mathbb{F}_1[x]$ is G-invariant. Indeed, if this is the case, then for an arbitrary $g \in G$, the the g^{-1}-image of the polynomial $\pi(x) = x$ is an element of $\mathbb{F}_1[x]$, and thus there exist $c, d \in \mathbb{F}$ such that $\pi^{g^{-1}}(x) = cx + d$. If we evaluate this polynomial equality at an arbitrary $\alpha \in \mathbb{F}$, we see that $\pi^{g^{-1}}(\alpha) = c\alpha + d$. On the other hand, the left-hand side of the quality equals $\pi(\alpha^g) = \alpha^g$. We have thus shown that for every $g \in G$, there exist $c, d \in \mathbb{F}$ such that $g\colon \alpha \mapsto c\alpha + d$ for every $\alpha \in \mathbb{F}$. Since g is a permutation of $\mathbb{F}$, we see that $c \neq 0$, and the result follows.

The rest of the proof is thus devoted to the proof that the subspace $\mathbb{F}_1[x]$ of $\mathbb{F}_{p-1}[x]$ is G-invariant.

For $r \in \{0, 1, \ldots, p-1\}$, let $M_r = \mathbb{F}_r[x]$. Let us first prove that the only non-trivial P-invariant subspaces of $\mathbb{F}_{p-1}[x]$ are M_r for $0 \leq r \leq p-1$. To this end, introduce the $\mathbb{F}$-linear transformation

$$\triangle\colon \mathbb{F}_{p-1}[x] \to \mathbb{F}_{p-1}[x],\ \ \triangle\colon f \mapsto f^{\rho} - f;$$

that is, $(\triangle f)(x) = f(x+1) - f(x)$. Now observe that, if f is of degree r, then $\triangle f$ is of degree (exactly) $r - 1$ (here the zero polynomial is treated as the polynomial of degree -1). This implies (PROVIDE DETAILS) that every non-trivial $\triangle$-invariant subspace of $\mathbb{F}_{p-1}[x]$ is one of M_r, $0 \leq r \leq p-1$.

Now observe that ρ (as a linear transformation of $\mathbb{F}_{p-1}[x]$) commutes with $\triangle$ and that every P-invariant subspace is also $\triangle$-invariant (indeed, since $\triangle = \rho - \mathrm{id}$), implying that the P-invariant subspaces of M_{p-1} are precisely M_r, as claimed.

Now observe that $M_{-1} = \langle 0 \rangle$, M_0 (constants) and M_{p-1} are also G-invariant. Moreover, $\{f \in \mathbb{F}_{p-1}[x] : \sum_{\alpha \in \mathbb{F}} f(\alpha) = 0\}$ is also a G-invariant subspace of codimension 1 (and must thus equal M_{p-2}).

Suppose now that for some r, $0 \leq r \leq p-3$, both M_r and M_{r+1} are G-invariant. Then $M_{r+1} : M_r = \{f \in \mathbb{F}_{p-1}[x] : fM_r \leq M_{r+1}\}$ (here the multiplication must be understood pointwise, that is, if the polynomials in fM_r that are of degree higher that $p-1$ must be first interpreted as functions and then the corresponding polynomials of degree at most $p-1$ must be found) is also G-invariant (CHECK!), and equals M_1 (CHECK!). (WHY DOES THIS ARGUMENT FAIL WHEN $r = p-2$?) Hence M_1 is G-invariant and the result follows.

We shall now assume that G is not double transitive and show that such an r indeed exists. Take $\varphi \in \mathrm{Hom}_G$ and $f \in \mathbb{F}_{p-1}[x]$, and show that $\varphi(\triangle f) = \triangle\varphi(f)$.

Now suppose that there exists $\varphi \in \mathrm{Hom}_G$ such that $\mathrm{Im}(\varphi) = M_t$ for some $t \in \{1, 2, \ldots, p-2\}$. Then let $r = t-1$ and observe that $\varphi(M_{p-2}) = \varphi(\triangle M_{p-1}) = \triangle\varphi(M_{p-1}) = \triangle M_t = M_r$. Now, since φ (as an element of Hom_G) maps G-invariant subspaces to G-invariant subspaces, both M_r and M_{r+1} are G-invariant, and the result follows.

To conclude the proof, it thus suffices to show that such a φ exists. To this end, take $f \in \mathbb{F}_{p-1}[x]$ of degree precisely $p-1$ (say $f(x) = x^{p-1}$). Then $\{f, \triangle f, \triangle^2 f, \ldots, \triangle^{p-1} f\}$ forms a basis for $\mathbb{F}_{p-1}[x]$. Use this to show that $\Psi\colon \mathrm{Hom}_G \to \mathbb{F}_{p-1}[x]$, $\varphi \mapsto \varphi(f)$, is injective and $\mathbb{F}$-linear. Now recall that, since G is doubly transitive, we have $\dim_{\mathbb{F}} \mathrm{Hom}_G \geq 3$. In particular, $\mathrm{Im}\Psi$ must contain a polynomial of degree t for some $t \in \{1, \ldots, p-2\}$ (WHY?). That is, there exists $\varphi \in \mathrm{Hom}_G$ such that $\varphi(f)$ has degree $t \in \{1, \ldots, p-2\}$. Since φ commutes with $\triangle$ and since $\mathbb{F}_{p-1}[x]$ is spanned by $\{f, \triangle f, \triangle^2 f, \ldots, \triangle^{p-1} f\}$, it follows that $\mathrm{Im}\varphi$ is spanned by $\{\varphi(f), \triangle\varphi(f), \triangle^2\varphi(f), \ldots, \triangle^{p-1}\varphi(f)\}$, and thus $\mathrm{Im}\varphi \leq M_t$. But on the other hand, $\mathrm{Im}\varphi$ is a G-invariant subspace containing a polynomial of degree t, implying that $\mathrm{Im}\varphi = M_t$. This proofs the theorem.